II. CLAIM AMENDMENTS

1. (Previously Presented) A method for generating a PIN, comprising:

generating a number of random binary bits;

determine the least significant bits of said number of bits;

converting the least significant bits to a decimal integer;

shifting the values of the integer by a predetermined constant to produce a shifted integer; and

encoding the shifted integer as bits in a PIN block.

2. (Previously Presented) The method of claim 1 wherein the shifted integer is encoded in accordance with encoding standard ISO 9564-1.

3. (Original) The method of claim 1, wherein the number of random bits is sixty-four.

4. (Original) The method of claim 1, wherein the number of least significant bits is sixteen.

5. (Original) The method of claim 1, wherein the constant is 173845.

6. (Original) The method of claim 1 wherein the PIN block includes:

a control field;

a PIN length designation field;

a series of PIN digit field;

at least one PIN/transaction digit; and

a series of transaction digit fields.

7. (Original) The method of claim 6, wherein each PIN digit field represents a binary number having a decimal value of from zero to nine.

8. (Original) The method of claim 6, wherein the control field is the binary number 0001.

9. (Original) The method of claim 6, wherein the PIN length field contains a binary number having a decimal value of four, five or six.

10. (Original) The method of claim 6, wherein the at least one PIN/transaction digit is determined in accordance with PIN length.

11. (Original) The method of claim 6, wherein the transaction digit fields are each four bit binary fields representing a decimal digit of zero to nine.

12. (Original) The method of claim 1 wherein the generating of the number of random binary bits is done by using a pseudo random number generator.

13. (Previously Presented) A method for managing security of a PIN used to provide access to a secure device, comprising:

choosing the PIN by:

generating a number of random binary bits;

determining the least significant bits of the number of random binary bits;

converting the least significant bits to a decimal integer;

shifting the values of the integer by a predetermined constant to produce a shifted integer; and

encoding the shifted integer as bits in a PIN block in accordance with an encoding standard;

the method also including:

storing an encrypted version of the PIN in the device; and

communicating the PIN to a user of the device via a first communication channel separate and apart from a second communication channel used to provide the device to the user.

14. (Previously Presented) The method of claim 13, wherein the first communication channel is a secure channel.

15. (Original) The method of claim 14, further comprising using encryption to render said communication channel secure.

16. (Original) The method of claim 13, wherein the user of said device chooses said PIN.

17. (Original) The method of claim 16, wherein a manufacturer of said device causes said encrypted version of said PIN to be stored in said device.

18. (Original) The method of claim 17, further comprising the manufacturer retaining a record of said PIN.

19. (Original) The method of claim 17, further comprising said manufacturer discarding all records of said PIN.

20. (Original) The method of claim 13 wherein said PIN is chosen using a random process.

21. (Cancelled)

22. (Previously Presented) The method of claim 13, wherein a manufacturer of said device causes said encrypted version of said PIN to be stored in said device.

23. (Original) The method of claim 22, further comprising the manufacturer retaining a record of said PIN.

24. (Original) The method of claim 22, further comprising said manufacturer discarding all records of said PIN.

25. (Original) The method of claim 13, wherein said device stores the value of funds.

26. (Original) The method of claim 13, wherein said device is a postal security device.

27. (Withdrawn) A method for resetting a PIN in a secure device comprising:

sending a message to a data center having an original PIN for said device, said message including authorization data indicative of the device and an authorized user of said device,

informing the authorized user of a remaining number of reset operations, and

securely communicating the original PIN to the location of the device.

28. (Withdrawn) The method of claim 27, wherein the device has a current PIN, further comprising replacing the current PIN with the original PIN.

29. (Withdrawn) The method of claim 27, wherein the communicating of the original PIN comprises:

sending the original PIN to the user of the device; and

the user of the device entering the original PIN into the device.

30. (Withdrawn) The method of claim 27 wherein at least one of sending a message to a data center and securely communicating the original PIN are performed using at least one of a secure communication channel and secure communication techniques.